PATENT

RECEIVED
CENTRAL FAX CENTER
FEB 2 2 2011

Remarks/Arguments

Claims 1, 3 - 9 are pending. No amendments have been made to these claims in this response.

Rejection of claims 1, 3 - 8 under 35 USC §102(e) as being anticipated by Hanson et al (U.S. Patent Application Publication No. 2002/0098840, hereinafter Hanson)

Applicants submit that for at least the reasons below, claim 1 is not anticipated by Hanson.

Hanson pertains to providing a seamless connection for nomadic mobile devices that are intermittently connected to a network. As the mobile device moves around, the device may lose its network connection or the device may be disconnected from it. In either case, the mobile device loses its ability to communicate with other devices connected to that network and loses its ability to receive any pending communications from them. In order to re-establish a network connection, the user of the device has to log in, determine where it left and recover any lost data (Hanson, paragraph [0016]).

The system of Hanson solves this problem by providing a seamless connection for these nomadic devices which involves the use of a centralized server, referred to as the Mobility Management Server (MMS). The MMS is connected to a mobile interconnect network that maintains the state of each Mobile End System (MES). The MMS handles the complex session management required to maintain persistent connections to the network and to other processes running on other peer networks. If the MES becomes unreachable, perhaps due to roaming from one network interconnect to another, the MMS acts as a proxy maintaining the network connection and acknowledging receipt of data and queuing requests intended for the unreachable MES (Hanson, paragraph [0023]).

A Remote Procedure Call (RPC) protocol in combination with an Internet Mobility Protocol is used to establish the seamless communication between the MMS and each MES. The RPC is used to generate messages from the network transactions intended for the disconnected device which are forwarded to the

MES. The MMS handles the transactions as a proxy for the disconnected MES. In this manner, the MMS does not lose any transactions as a result of being disconnected from the network.

By contrast, the claimed invention pertains to trust relationships. Trust is based on the fact that a trusted device will not act maliciously. A device builds a trusted relationship with another device through the use of a provable identity (paragraph [0045]). A provable identity can be a secure mechanism such as public/private key pair (paragraph [0081]). Once a device establishes a trust relationship with another device, the trust relationships are stored within the device. The trust relationships are used to form a community of devices within a network that are secure from malicious acts. The trust relationships are synchronized with each device in the community. This synchronization ensures that an untrusted device is removed from the community quickly (paragraph [0076]). The trust relationships are established to allow the transitivity of the trust relationships throughout the community without any user intervention or with the use of a central device, such as the MMS.

The concept of trust relationships of the claimed invention is clearly distinguishable from the seamless connection of devices to networks in Hanson. Hanson pertains to maintaining a seamless connection for mobile devices that roam from one coverage zone to another. The seamless connection between a mobile device and a network interconnect differs from a trust relationship. In Hanson, a mobile device may roam into a coverage zone and connect to a network that may have malicious devices (i.e., untrusted devices) connected to it. Since Hanson pertains to a different problem than the claimed invention, Hanson does not recite the trust relationships found in the claimed invention.

Claim 1 recites the following:

> 1. A device adapted to belong to a community of networked devices, said device comprising:
> a provable identity and/or means for generating and/or obtaining a provable identity;

> *means adapted to store information about devices*
> *of the community having trust relationships with said device;*
>   *means adapted to store information about devices*
> *of the community having had trust relationships with said*
> *device in the past but now not trusted by said device;*
>   *means for trust relationships synchronization with*
> *each device belonging to said community of network devices*
> *based on the stored information.*

The Examiner contends that the bold-highlighted elements are recited in Hanson. Applicants respectfully disagree.

The Examiner contends that the *"means adapted to store information about devices of the community having trust relationships with said device"* is recited in Hanson in paragraph [0096], lines 1-6.

Paragraph [0096], lines 1 -6 recites the following:

"For example, server 102 allows any conventional (e.g., TCP/IP based) network application to operate without modification over mobile connection. Server 102 maintains the session of Mobile End Systems 104 that disconnect, go out of range or suspend operation, and resumes the sessions when the Mobile End System returns to service."

This cited section indicates that a session on the MES is maintained on the server in the event the MES is disconnected from the network. By contrast, the *"means adapted to store information about devices of the community having trust relationships with said device"* pertains to storing trust relationships. As noted above, a trust relationship differs from maintaining a mobile session with a server which is why the above feature is not recited in Hanson.

The Examiner contends that the *"means adapted to store information about devices of the community having had trust relationships with said device in the past but now not trusted by said device"* is recited in Hanson at paragraph [0218], lines 10-18. Applicants respectfully disagree.

PATENT

Paragraph [0218], lines 10 – 18 recites the following:

"If the specified period of time expires without any activity from
the Mobile End System 104, the Mobility Management Server 102
may terminate a session. Also, an administrator may want to limit
the overall time a particular connection may be established for, or
when to deny access base on time of day. Again these policy timers
may, in one example implementation, be invoked only on the Mobility
Management Server 102 side."

This cited section does not recite trust relationships or a means to store
information about devices in the community having had a previous trust
relationships. Rather, the cited section indicates that the server of Hanson can
terminate a session based on inactivity from a device (e.g., MES) or due to
expiration of a timer. Clearly, this differs from storing information on which devices
are no longer trusted despite having been trusted previously.

The Examiner contends that the *"means for trust relationships
synchronization with each device belonging to said community of network devices
based on the stored information"* is recited in Hanson at paragraph [0099], lines 1 -
12. Applicants respectfully disagree.

Paragraph [0099], lines 1 – 12 recites the following:

*"A Mobile End System 104 establishes an association with the
Mobility Management Server 102, either at startup or when the
Mobile End System requires network services. Once this association
is established, the Mobile End System 104 can start one or more
network application sessions, either serially or concurrently. The
Mobile End System 104-to-Mobility Management Server 102
association allows the Mobile End System to maintain application
sessions when the Mobile End System, disconnects, goes out of
range or suspends operation, and resume sessions when the Mobile
End System returns to service. In the preferred embodiment, this
process is entirely automatic and does not require any intervention
on the user's part."*

The cited section above pertains to establishing a connection or association between a MES and the MMS. The connection is essential for the server to handle the MES's session in the event the MES loses its physical network connection. However, this cited section does not recite synchronizing trust relationships. The synchronization of trust relationship enables two devices to form a trust relationship if they have a trust relationship with a common third device. Accordingly, the cited section does not recite "*means for trust relationships synchronization with each device belonging to said community of network devices based on the stored information.*"

In view of the above, Applicants submit that claim 1 is not anticipated by Hanson. Claims 3 – 8 depend on claim 1 and are not anticipated by Hanson by virtue of their dependence on claim 1.

Rejection of claim 9 under 35 USC §103(a) as being unpatentable over Hanson as applied to claim 6, in view of Fraser et al (U.S. Patent Pub. No. 2003/0131232).

Applicants respectfully traverse this rejection since Fraser is unable to remedy the deficiencies of Hanson explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

PATENT

RECEIVED
CENTRAL FAX CENTER

FEB 2 2 2011

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited.

It is believed that there are no additional fees due with regard to the filing of this response. However if there is an additional fee due, please charge the fee, or credit any overpayment, to Deposit Account No. 07-0832.

Respectfully submitted,
NICHOLAS PRIGENT ET AL.

By:

Paul P. Kiel, Attorney
Reg. No. 40,677
Phone (609) 734-6815

Date: 2/22/11

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08543-5312

9